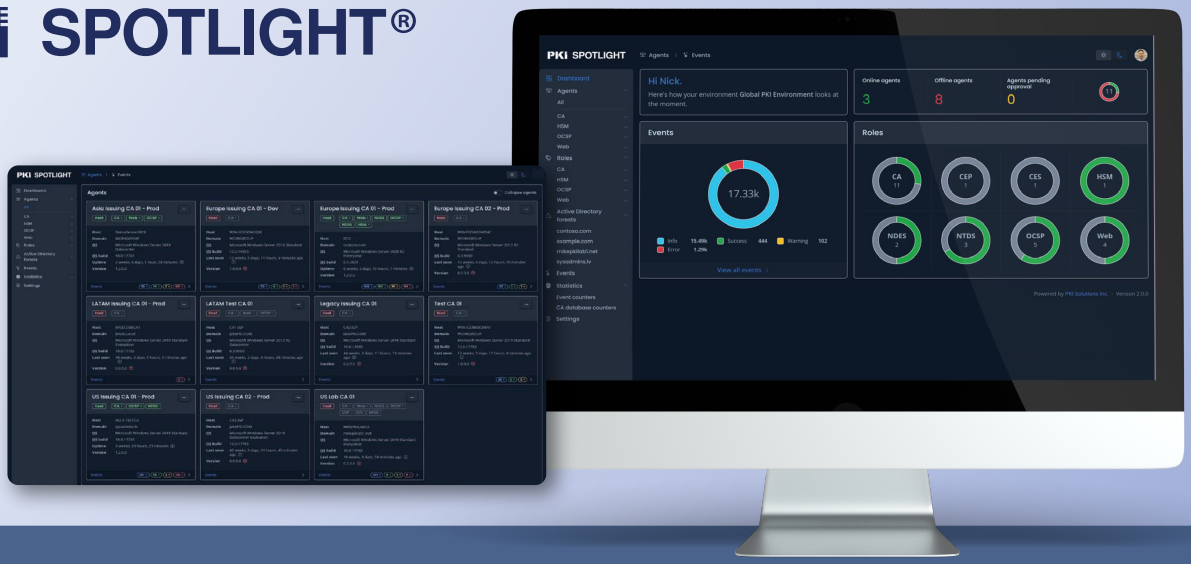
PKI SPOTLIGHT®



See the Unseen

Near real-time monitoring and alerting of the availability, configuration, and security of Microsoft and non-Microsoft PKI and HSM environments - consolidated, and at your fingertips.

Why?

The distributed nature of Public Key Infrastructure (PKI) poses operational challenges that are not addressed by certificate lifecycle management or monitoring products. Most organizations struggle to manage their PKIs.

These factors increase an organization's risk to business disruption, lurking threats, and chances of making the news for the wrong reasons.

OPERATIONAL RESILIENCE

Improve your Microsoft and non-Microsoft PKIs and Hardware Security Modules (HSM) uptime and availability.

SECURITY POSTURE MANAGEMENT

Maintain the security and integrity of your PKI with visibility into configurations that can impact identity and encryption systems.

THREAT DETECTION

Protect your PKI against malicious activity. Quickly spot any abnormal activity, vulnerabilities, and exploitable misconfigurations in your PKI environments.

BEST PRACTICES INCLUDED

By Design: Review and refine your PKI operational and configuration practices.

CORE CAPABILITIES

Near real-time PKI and HSM monitoring for critical PKI functions, events, activity, and configuration changes with support for Microsoft ADCS and HashiCorp Vault.

Integration with Splunk for streaming of events, best practice alerts, and threat alerts.

Event and alert notifications via individual and digest email subscriptions to support Incident/Service Management and day-to-day operations.

More than 100 pre-configured rules to continually check the status of PKI and events against security and operational best practices for Online and Offline Certificate Authority (CA), Certificate Authority Web Enrollment (CAWE), Network Device Enrollment Service (NDES), Host, and Online Certificate Status Protocol (OCSP) configurations.

Detection and remediation recommendations for best practices and threats from vulnerabilities, including PetitPotam and the exploits identified in the SpecterOps "Certified Pre-Owned: Abusing Active Directory Certificate Services" white paper.

A centralized dashboard that shows active PKI component service status, events, detected vulnerabilities, and best practice alerts.

A topology view to quickly asses PKI status.

REQUEST A DEMO!

PKISPOTLIGHT.COM

+1 971 231-5523 hello@pkisolutions.com

PKI SPOTLIGHT®

Best Practices

Keep up with the best practices required to keep your PKIs and HSMs functional, available, and secure.

- Align PKI component configurations with organizational or industry standards.
- Leverage Best Practices to identify and prioritize high-value improvements to PKI and HSM configurations.
- Centralized dashboard to ensure components are configured and operating per design
- Support for running Best Practices against off-network CAs

Operational Resilience

With consolidated PKI-wide system configuration and events at their fingertips, PKI admins and operations teams can at any time.

- Check events for signs of availability, pre-failure, and failover states
- Get alerts on CA's ability to sign requests
- Get alerted on CRL errors and detect pre-failure CRL states, including pending expirations
- Checklist of dependencies to detect pre-failure conditions and to ensure that the CA is servicing requests.
- Scheduled and automated granular health checks on NDES and associated IIS servers
- Stay on top of Microsoft NDES availability and HashiCorp Vault
- Verify against desired operational state across network segments and Microsoft Active Directory forests
- Get notified of any PKI-related service shutdown events

LEARN MORE!
PKISPOTLIGHT.COM

THREAT DETECTION

Protect your PKI against malicious activity. Quickly spot any abnormal activity, vulnerabilities, and exploitable misconfigurations in your PKI environments.

- Near real-time alerts on the presence of PKI vulnerabilities and for exploitable Certificate Template misconfigurations
- View unusual CA permission and revocation activities
- Identify out-of-the-ordinary activities in PKI-related Active Directory containers and cryptography
- Visibility into CA Certificates that are published and trusted in Active Directory
- Checks for exploitable certificate template misconfigurations to prevent escalation of privileges and man-in-the-middle attacks

SECURITY POSTURE MANAGEMENT

Identify misconfiguration issues that affect the security and integrity of identity, access, and data.

- View Hardware Security Module (HSM) configurations
- View Cryptographic provider configurations
- View Service Principal Names (SPN) and TLS bindings for Microsoft NDES IIS application pools
- View Certificate Revocation Checking configurations
- Password and dynamic password enforcement for all Microsoft NDES roles
- View Key Recovery Agent status and configurations
- View PKI Server Firewall modifications and current operational state